On the number of n-ary quasigroups of finite order*

V. N. Potapov*, D. S. Krotov*

**Sobolev Institute of Mathematics, prospect Akademika Koptyuga 4, Novosibirsk*
Mechanics and Mathematics Department of the Novosibirsk State University, Pirogova 2, Novosibirsk

Abstract

Let $Q(n,k)$ be the number of n-ary quasigroups of order k. We derive a recurrent formula for $Q(n,4)$. We prove that for all $n \geq 2$ and $k \geq 5$ the following inequalities hold: $\left(\frac{k-3}{2}\right)^{\frac{n}{2}} \left(\frac{k-1}{2}\right)^{\frac{n}{2}} < \log_2 Q(n,k) \leq c_k(k-2)^n$, where c_k does not depend on n. So, the upper asymptotic bound for $Q(n,k)$ is improved for any $k \geq 5$ and the lower bound is improved for odd $k \geq 7$.

Keywords: n-ary quasigroup, latin cube, loop, asymptotic estimate, component, latin trade.

UDC: 519.143
MSC2010: 20N15, 05B15

1. Introduction

An algebraic system from a set Σ of cardinality $|\Sigma| = k$ and n-ary operation $f : \Sigma^n \to \Sigma$ is called an n-ary quasigroup of order k iff the unary operation obtained by fixing any $n-1$ arguments of f by any values from Σ is always bijective. The corresponding function f is often also called an *n-ary quasigroup* (the value table of such a function is known as *latin hypercube*; if $n = 2$, *latin square*).

Let us fix the set $\Sigma = \{0, 1, \ldots, k-1\}$. Denote by $Q(n,k)$ the number of different n-ary quasigroups of order k (for fixed Σ)[1]. It is known that for every n there exist only two n-ary quasigroups of order 2. There are exactly $Q(n,3) = 3 \cdot 2^n$ different n-ary quasigroups of order 3, which form one equivalence class. In [9] it is proved that $Q(n,4) = 3^{n+1}2^{2^n+1}(1+o(1))$ as $n \to \infty$. In Section 4 we suggest a recurrent way to calculate the numbers $Q(n,4)$ and list the first 8 values. Before, only five values of $Q(n,4)$ where known; furthermore the numbers $Q(n,5)$ and $Q(n,6)$ are known for $n \leq 5$ and $n \leq 3$ respectively, see [7], and the number $Q(2,k)$ for $k \leq 11$, see [6] and references there.

The asymptotics of the number and even of the logarithm of the number (and even of the logarithm of the logarithm of the number) of n-ary quasigroups of orders more than 4 is unknown. In [5], the following lower bounds are derived: $Q(n,5) \geq 2^{3^{n/3}-c}$, where $c < 0.072$; $Q(n,k) \geq 2^{(k/2)^n}$ if k is even; $Q(n,k) \geq 2^{n(k/3)^n}$ if $k \equiv 0 \bmod 3$; $Q(n,k) \geq 2^{1.5\lfloor k/3 \rfloor^n}$ for an arbitrary k. The following upper bound was established in [8]: $Q(n,k) \leq 3^{(k-2)^n} 2^{n(k-2)^{n-1}}$.

*This work was partially supported by the Federal Target Program "Scientific and Educational Personnel of Innovation Russia" for 2009-2013 (contract No. 02.740.11.0429) and the Russian Foundation for Basic Research (grants 08-01-00671, 08-01-00673).

[1]Sometimes by the number of quasigroups one mean the number of mutually nonisomorphic quasigroups.

In this paper we improve the upper bound (Section 2) on the number of n-ary quasigroups of finite order and the lower bound (Section 3) on the number of n-ary quasigroups of odd order:

$$\left(\frac{k-3}{2}\right)^{\frac{n}{2}}\left(\frac{k-1}{2}\right)^{\frac{n}{2}} < \log_2 Q(n,k) \le c_k(k-2)^n,$$

where c_k does not depend on n; explicitly, $c_k = \frac{\log_2 k!}{k-2} + \frac{k}{k-4}$.

2. An upper bound

We will say that a set $M \subseteq \Sigma^n$ satisfies Property (A) iff for every element $\bar{x} \in M$ and every position $i = 1, \ldots, n$ there is another element $\bar{y} \in M$ differing from $\bar{x}$ only in the position i. By induction it is easy to get the following:

Proposition 1. *Any nonempty subset $C \subseteq \Sigma^n$ that satisfies Property (A) has the cardinality at least 2^n.*

A function $g : \Omega \to \Sigma$ where $\Omega \subset \Sigma^n$ is called a *partial n-ary quasigroup of order $|\Sigma|$* if $g(\overline{x}) \neq g(\overline{y})$ for any two tuples $\overline{x}, \overline{y} \in \Omega$ differing in exactly one position. We will say that an n-ary quasigroup $f : \Sigma^n \to \Sigma$ is an *extension* of a partial n-ary quasigroup $g : \Omega \to \Sigma$ where $\Omega \subset \Sigma^n$ if $f|_\Omega \equiv g$.

Lemma 1. *Let $|\Sigma| = k$, $B = \Sigma \setminus \{a, b\}$, $k \ge 3$, $a, b \in \Sigma$. Then a partial n-ary quasigroup $g : \Sigma^{n-1} \times B \to \Sigma$ has at most $2^{(k/2)^{n-1}}$ different extensions.*

Proof. Denote by P the set of the unordered pairs of elements of Σ. Consider a partial n-ary quasigroup $g : \Sigma^{n-1} \times B \to \Sigma$. Define the function $G : \Sigma^{n-1} \to P$ by the equality $G(\overline{x}) = \Sigma \setminus \{g(\overline{x}c) : c \in \Sigma \setminus \{a, b\}\}$. Define the graph $\Gamma = \langle \Sigma^{n-1}, E\rangle$ where two vertices $\overline{x}$ and $\overline{y}$ are adjacent if and only if the tuples $\overline{x}$ and $\overline{y}$ differ in exactly one position and $G(\overline{x}) \cap G(\overline{y}) \neq \varnothing$. It is easy to see that connected components of Γ satisfy Property (A).

Let n-ary quasigroups f_1 and f_2 be extensions of g. It is not difficult to see that $\{f_1(\overline{x}a), f_1(\overline{x}b)\} = G(\overline{x})$ for every $\overline{x} \in \Sigma^{n-1}$; moreover, if $f_1(\overline{x}a) = f_2(\overline{x}a)$, then f_1 and f_2 coincide on the whole connected component of Γ containing $\overline{x} \in \Sigma^{n-1}$. So, to define an extension of g uniquely it is sufficient to choose one from the two possible values for every connected component of Γ. It follows from Proposition 1 that every connected component has cardinality at least 2^{n-1}. Then the number of connected components of Γ does dot exceed $(k/2)^{n-1}$. Hence g has not more than $2^{(k/2)^{n-1}}$ extensions. ▲

Theorem 1. *If $k \ge 5$ and $n \ge 2$ then $Q(n,k) \le 2^{c_k(k-2)^n}$, where $c_k = \frac{\log_2 k!}{k-2} + \frac{k}{k-4}$.*

Proof. The number of partial n-ary quasigroups $g : \Sigma^{n-1} \times B \to \Sigma$, where $|\Sigma| = k$, $B = \Sigma \setminus \{a, b\}$, does not exceed $Q(n,k)^{k-2}$. From Lemma 1 we have

$$Q(n+1,k) \le Q(n,k)^{k-2} 2^{(k/2)^n}. \tag{1}$$

Denote $\alpha_n = \log_2 Q(n,k)/(k-2)^n$. Then from (1) we have

$$\alpha_{n+1} \le \alpha_n + \left(\frac{k}{2(k-2)}\right)^n.$$

Since $\alpha_1 = \frac{\log_2 k!}{k-2}$ and $\sum\limits_{n=1}^{\infty}\left(\frac{k}{2(k-2)}\right)^n = \frac{k}{k-4}$, we get $\alpha_n \le \frac{\log_2 k!}{k-2} + \frac{k}{k-4}$. ▲

3. A lower bound

Let a and b be two different elements of Σ. By $\{a,b\}$-*component* of an n-ary quasigroup f we will mean such a set $S \subset \Sigma^n$ that 1) $f(S) = \{a,b\}$ and 2) the function

$$g(\bar{x}) = \begin{cases} f(\bar{x}) & \text{whenever } \bar{x} \notin S, \\ b & \text{whenever } \bar{x} \in S \text{ and } f(\bar{x}) = a, \\ a & \text{whenever } \bar{x} \in S \text{ and } f(\bar{x}) = b \end{cases}$$

is also an n-ary quasigroup. In this case we will say that g is obtained from f by *switching* the component S. We note that in the definition of an $\{a,b\}$-component the condition 2) can be replaced by Property (A) from the previous section. It is obvious that switching disjoint components can be performed independently:

Proposition 2. *Let S and S' be disjoint $\{a,b\}$- and $\{c,d\}$- (respectively) components of an n-ary quasigroup f. Let an n-ary quasigroup g is obtained from f by switching S. Then S' is a $\{c,d\}$-component of g too.*

The following proposition can be easily derived from the definition of an $\{a,b\}$-component; similar statement can be found in [5].

Proposition 3. *Let $C = \{c_1,d_1\} \times \{c_2,d_2\}$ be an $\{a,b\}$-component of a 2-ary quasigroup g. Let C_i be a $\{c_i,d_i\}$-component of an n_i-ary quasigroup q_i, $i = 1,2$. Then the set $C_1 \times C_2$ is an $\{a,b\}$-component of the (n_1+n_2)-ary quasigroup f, where $f(\bar{x}_1,\bar{x}_2) \equiv g(q_1(\bar{x}_1), q_2(\bar{x}_2))$.*

A 2-ary quasigroup $\varphi : \Sigma \to \Sigma$ is called *idempotent* iff $\varphi(x,x) = x$ for every $x \in \Sigma$. It is known (see, e.g., [1]) that

Proposition 4. *For every $m \geq 3$ there exists an idempotent 2-ary quasigroup of order m.*

The following proposition presents a construction of 2-ary quasigroups, which will be used to establish a lower bound on the number of n-ary quasigroups of odd order.

Proposition 5. *For any $m \geq 3$ there exists a 2-ary quasigroup ψ of order $2m+1$ that has m $\{2i,2i+1\}$-components for every $i \in \{0,\ldots,m-1\}$; moreover, all except one $\{2i,2i+1\}$-components have form $\{2j,2j+1\} \times \{2l,2l+1\}$.*

Proof. By Proposition 4 there exists an idempotent 2-ary quasigroup φ_m of order m. For each $a,b \in \{0,\ldots,m-1\}$, $a \neq b$, and $\delta,\sigma \in \{0,1\}$ define

$\psi(2a+\delta, 2b+\sigma) = 2\varphi_m(a,b) + (\delta+\sigma \bmod 2)$;

$\psi(2a+\delta, 2a+\delta) = 2a+1-\delta$;

$\psi(2a+\delta, 2a+1-\delta) = k-1$;

$\psi(k-1, 2a+\delta) = \psi(2a+\delta, k-1) = 2a+\delta$;

$\psi(k-1, k-1) = k-1$.

Straightforwardly, ψ is a 2-ary quasigroup that satisfied the desired properties. ▲

The following is examples of the value tables of a 2-ary quasigroup φ_4 and the corresponding ψ:

φ_4 :

0	2	3	1
3	1	0	2
1	3	2	0
2	0	1	3

ψ :

1	8	4	5	6	7	2	3	0
8	0	5	4	7	6	3	2	1
6	7	3	8	0	1	4	5	2
7	6	8	2	1	0	5	4	3
2	3	6	7	5	8	0	1	4
3	2	7	6	8	4	1	0	5
4	5	0	1	2	3	7	8	6
5	4	1	0	3	2	8	6	7
0	1	2	3	4	5	6	7	8

From Proposition 1 it is easy to conclude that the odd-order 2-ary quasigroup constructed in Proposition 5 has the maximal number of mutually disjoint components among all 2-ary quasigroups of the same order.

Theorem 2. *If k is an odd integer ,$k \geq 5$, and $n \geq 2$, then*

$$Q(n,k) \geq 2^{\left(\frac{k-3}{2}\right)^{\left\lfloor \frac{n-1}{2} \right\rfloor}\left(\frac{k-1}{2}\right)^{\left\lceil \frac{n+1}{2} \right\rceil}} > 2^{\left(\frac{k-3}{2}\right)^{n/2}\left(\frac{k-1}{2}\right)^{n/2}}.$$

Proof. Let ψ be the 2-ary quasigroup of order k constructed in Proposition 5. Define the n-ary quasigroup Ψ^n by the following recurrent equalities:

$\Psi^2 \equiv \psi$;

$\Psi^{2m+1}(\overline{x}, y) = \psi(\Psi^{2m}(\overline{x}), y)$;

$\Psi^{2m+2}(\overline{x}, y, z) = \psi(\Psi^{2m}(\overline{x}), \psi(y, z))$.

Denote by α_n the number of $\{2i, 2i+1\}$-components of Ψ^n where $i \in \{0, \ldots, \frac{k-3}{2}\}$. From Propositions 3 and 5 we have the relations $\alpha_2 = \frac{k-1}{2}$, $\alpha_{2m+1} \geq \alpha_{2m}\frac{k-3}{2}$, $\alpha_{2m+2} \geq \alpha_{2m}\frac{k-3}{2}\frac{k-1}{2}$. Then $\alpha_{2m} \geq \left(\frac{k-3}{2}\right)^{m-1}\left(\frac{k-1}{2}\right)^{m}$ and $\alpha_{2m+1} \geq \left(\frac{k-3}{2}\right)^{m}\left(\frac{k-1}{2}\right)^{m}$.

Since $\{2i, 2i+1\}$-components with different i are disjoint, the number of disjoint components is at least $\frac{k-1}{2}\alpha_n$. From Proposition 2 we deduce that we can get the desired number of different n-ary quasigroups of order k by switching disjoint components in Ψ^n. ▲

4. The number of different n-ary quasigroups of order 4

Denote $[n] = \{1, \ldots, n\}$. An n-ary quasigroup f is called an *n-ary loop* iff there exists an element $e \in \Sigma$, which is called an *identity*, such that for all $i \in [n]$ and $a \in \Sigma$ it is true $f(e \ldots e\underset{i}{a}e \ldots e) = a$. In what follows we always assume that 0 is an identity of an n-ary loop (in general, an n-ary loop can have more than one identities provided $n \geq 3$). Especially we note that this agreement is essential in the treatment of the concept of the number of n-ary loops. In particular, we have the following simple and well-known fact:

Proposition 6. *Let $Q'(n,k)$ be the number of n-ary loops of order k. Then* $Q(n,k) = k \cdot ((k-1)!)^n Q'(n,k)$.

An n-ary quasigroop f is called *permutably reducible* (we will omit "permutably") iff there exist an integer m, $2 \leq m < n$, an $(n-m+1)$-ary quasigroup h, an m-ary quasigroup g , and a permutation $\sigma : [n] \to [n]$ such that

$$f(x_1, \ldots, x_n) \equiv h\left(g(x_{\sigma(1)}, \ldots, x_{\sigma(m)}), x_{\sigma(m+1)}, \ldots, x_{\sigma(n)}\right).$$

In this section we will assume that $\Sigma = \{0, 1, 2, 3\}$; i.e., we will consider only the n-ary quasigroups of order 4. It is known (see, e.g., [**?**]) that there are exactly four binary loops of order 4 (one is isomorphic to the group $Z_2 \times Z_2$ and three, to the group Z_4).

The following statement is straightforward from the theorem in [3].

Lemma 2. *Every reducible n-ary loop f of order 4 admits exactly one of the following two representations.*

$$f(\overline{x}) = q_0(q_1(\tilde{x}_1), ..., q_m(\tilde{x}_m)) \tag{2}$$

where q_j are n_j-ary loops; $\tilde{x}_j$ are tuples of variables x_i, $i \in I_j$, where $\{I_j\}$ is a partition of $[n]$, $j = 1, \ldots, m$; q_0 is an irreducible m-ary loop, $m \geq 3$. Moreover, the partition $\{I_j\}$ in such a representation is unique for every f.

$$f(\overline{x}) = q_1(\tilde{x}_1) * ... * q_k(\tilde{x}_k) \tag{3}$$

where $*$ is a binary operation in one of the 4 loops, q_j, $j = 1, \ldots, k$, are n_j-ary loops that are not representable in the form $q_j(\tilde{x}_j) = q'(\tilde{x}'_j) * q''(\tilde{x}''_j)$, $\tilde{x}_j$ are tuples of variables x_i, $i \in I_j$, where $\{I_j\}$ is a partition of $[n]$. Moreover, the partition $\{I_j\}$ in such a representation is unique for every f.

By the *root operation* of an n-ary quasigroup f we will mean the m-ary quasigroup q_0 if (2) holds, and the binary operation $*$ if (3) holds.

Simple combinatorial calculations give the following formula for the number $F_{\overline{j},\overline{k}}$ of different partitions of $[n]$ into k subsets from which exactly k_i subsets have cardinality j_i, $1 \leq i \leq t$, $0 < j_1 < \cdots < j_t$:

$$F_{\overline{j},\overline{k}} = \frac{n!}{(j_1!)^{k_1} \ldots (j_t!)^{k_t}} \frac{1}{k_1! \ldots k_t!}, \tag{4}$$

where $k_1 + k_2 + \cdots + k_t = k$, $k_1 j_1 + k_2 j_2 + \cdots + k_t j_t = n$.

Let $f : \Sigma^n \to \Sigma$ be an n-ary quasigroup; define the set

$$S_{a,b}(f) \triangleq \cup\{\bar{x} \in \Sigma^n : f(\bar{x}) \in \{a, b\}\}.$$

An n-ary loop f will be called *a-semilinear*, where $a \in \{1, 2, 3\}$, if the characteristic function $\chi_{S_{0,a}(f)}$ of the set $S = S_{0,a}(f)$ has the form

$$\chi_{S_{0,a}(f)}(x_1, \ldots, x_n) \equiv \sum_{i=1}^{n} \chi_{\{0,a\}}(x_i) \bmod 2. \tag{5}$$

An n-ary loop f is called *linear* if it is a-semilinear and b-semilinear for some different a and b from $\{1, 2, 3\}$. It is not difficult to check the following:

Proposition 7. *One of the four binary loops of order 4 is linear (the one that is isomorphic to $Z_2 \times Z_2$); the other three are 1-, 2-, and 3- semilinear respectively.*

It is known (see [9]) that

Proposition 8. *A linear n-ary loop is unique and is 1-, 2-, and 3- semilinear.*

It is not difficult to see (see also [9]) the following:

Proposition 9. *Let f be a reducible a-semilinear n-ary loop; then f can be represented as the composition (2) or (3) of a-semilinear loops.*

Let us denote by ℓ_n^a the number of the a-semilinear n-ary loops and by ℓ_n the number of the semilinear n-ary loops.

As established in [9], the number of the n-ary loops asymptotically coincides with ℓ_n, which can be easily calculated:

Lemma 3 ([9]). $\ell_n = 3 \cdot 2^{2^n-n-1} - 2$, $\ell_n^a = 2^{2^n-n-1}$ *for* $a \in \{1,2,3\}$.

In [4] the set of n-ary quasigroups of order 4 was characterized in the terms defined above; namely, the following was proved:

Theorem 3. *Every n-ary loop of order 4 is reducible or semilinear.*

This fact gives a base for deriving a recurrent formula for the number of n-ary loops (and quasigroups) of order 4.

We will use the following notation:

v_n is the number of the n-ary loops (of order 4);

r_n^* is the number of the reducible n-ary loops with the binary root operation $*$;

r_n^0 is the number of the reducible n-ary loops with the root operation of arity at least 3;

r_n^{a*} is the number of the reducible a-semilinear n-ary loops with the a-semilinear binary root operation $*$;

r_n^{a0} is the number of the reducible a-semilinear n-ary loops with the root operation of arity at least 3;

p_n^a is the number of irreducible a-semilinear n-ary loops;

p_n is the number of irreducible n-ary loops.

From Lemma 2 and Proposition 9, the following relations follow:

$$r_n^{a*} = \sum_{i=2}^{n} \sum_{\bar{j},\bar{k}} F_{\bar{j},\bar{k}} (\ell_{j_1}^a - r_{j_1}^{a*})^{k_1} \cdots (\ell_{j_t}^a - r_{j_t}^{a*})^{k_t},$$

$$r_n^* = \sum_{i=2}^{n} \sum_{\bar{j},\bar{k}} F_{\bar{j},\bar{k}} (v_{j_1} - r_{j_1}^*)^{k_1} \cdots (v_{j_t} - r_{j_t}^*)^{k_t},$$

$$r_n^{a0} = \sum_{i=3}^{n-1} p_i^a \sum_{\bar{j},\bar{k}} F_{\bar{j},\bar{k}} (\ell_{j_1}^a)^{k_1} \cdots (\ell_{j_t}^a)^{k_t},$$

$$r_n^0 = \sum_{i=3}^{n-1} p_i \sum_{\bar{j},\bar{k}} F_{\bar{j},\bar{k}} (v_{j_1})^{k_1} \cdots (v_{j_t})^{k_t},$$

where the second sum os over the tuples $\bar{k} = (k_1, \ldots, k_t)$ and $\bar{j} = (j_1, \ldots, j_t)$ of positive integers satisfying $k_1 + \cdots + k_t = i$, $k_1 j_1 + k_2 j_2 + \cdots + k_t j_t = n$ and $j_1 < \cdots < j_t$. From Theorem 3 and Proposition 8 we have $v_n = p_n + r_n^0 + 4r_n^*$, $p_n^a = \ell_n^a - r_n^{a0} - 2r_n^{a*}$, $p_n = 3p_n^a$. From Lemma 3, $\ell_n^a = 2^{2^n-n-1}$ for $a \in \{1,2,3\}$.

Proposition 7 gives the initial values $r_2^{a*} = 2$, r_2^*=4, $r_2^{a0} = r_2^0 = 0$. We see that the equalities above and Proposition 6 provide a recurrent way of calculation of the number of the n-ary quasigroups of order 4.

Finally, we list the first eight values of $Q'(n,4)$:

1,
4,
64,
7132,
201538000,
432345572694417712,
39876839873547476429227733539632779 68,
67846927287489958255998624028528071036486706348977951042703872222975027 6832,

and of $Q(n,4)$:
24,
576,
55296,
36972288,
6268637952000,
80686060158523011084288,
44651852187365545446769179264602567250000192,
45582713849161893490442953958520081824807862308417980087416842819065769638858260 48.

5. Conclusion

We will briefly discuss a connection of our topic with the known concept of latin traid. A partial n-ary quasigroup $t : \Omega \to \Sigma$, $\Omega \subset \Sigma^n$ is called a *multidimensional latin trade*, here for briefity simply *trade* iff there exist another partial n-ary quasigroup $t' : \Omega \to \Sigma$ such that

1) $t(\bar{x}) \neq t'(\bar{x})$ for all $\bar{x} \in \Omega$;

2) for any i from 1 to n and any admissible values x_1, ..., x_{i-1}, x_{i-1}, ..., x_n the sets $\{t(x_1, \ldots, x_{i-1}, y, x_{i-1}, \ldots, x_n) \mid y \in \Sigma\}$ and $\{t'(x_1, \ldots, x_{i-1}, y, x_{i-1}, \ldots, x_n) \mid y \in \Sigma\}$ coincide.

In this case the pair (t, t') is called a *bitrade* (depending on the context, bitrades are considered either as ordered, or as unordered pairs); the trade t' is called a *mate* of t. In the case $n = 2$ bitrades (latin bitrades) are widely studied, see the survey [2].

We will say that an n-ary quasigroup f has a trade t iff $t = f|_\Omega$ for some Ω. As follows from the definitions, replacing of the values of f in Ω by the values of a mate t' of t results in another n-ary quasigroup. We will say that trades $t = f|_\Omega$ and $s = f|_\Theta$ are *independent* iff their supports Ω and Θ are disjoint. The maximal number of mutually independent trades of an n-ary quasigroup f will be called its *trade number* $\mathrm{trd}(f)$. Denote by $\mathrm{Trd}(n,k)$ the maximum of $\mathrm{trd}(f)$ over the all n-ary quasigroups f of order k. Since independent trades of an n-ary quasigroup can be independently replaced by mates, the number $Q(n,k)$ of different n-ary quasigroups of order k satisfies

$$Q(n,k) \geq 2^{\mathrm{Trd}(n,k)}. \tag{6}$$

It is easy to understand that the lower bound in Section 3 (as well as all the bounds in [5]) is derived by this way: $\{a,b\}$-component is the support of some trade by definitions. Since the support of a trade satisfies Property (A), Proposition 1 implies $\mathrm{Trd}(n,k) \leq k^n/2^n = 2^{(\log_2 k - 1)n}$; moreover, for even k the equality is easily proved. For odd k, as follows from the results of Section 3, we have $\mathrm{Trd}(n,k) \geq 2^{c(k)n}$ where $c(k) \underset{k\to\infty}{\longrightarrow} \log_2 k - 1$. But for fixed k, in particular, for the small values 5, 7, ..., the question about the asymptotics of $\mathrm{Trd}(n,k)$ remains open.

Problem 1. *Establish the asymptotics of the logarithm and the asymptotics of the value* $\mathrm{Trd}(n,k)$ *as* $n \to \infty$ *for odd* $k \geq 5$.

Another question is how the estimation (6) close to the real value. For the order 4 it is asymptotically tight in logarithms. For any larger fixed order the asymptotics of $\log\log Q(n,k)$ is unknown. It is natural to conjecture that the asymptotics of $\log\log Q(n,k)$ and $\log \mathrm{Trd}(n,k)$ coincide.

Problem 2. *Is it true that* $\lim\limits_{n\to\infty} \left(\frac{\log_2 \log_2 Q(n,k)}{n}\right) = \lim\limits_{n\to\infty} \left(\frac{\log_2 \mathrm{Trd}(n,k)}{n}\right)$*? In particular, is it true that* $\lim\limits_{n\to\infty} \left(\frac{\log_2 \log_2 Q(n,k)}{n}\right) \leq \log_2 k - 1$*?*

Even the existence of these limits is not proved yet.

References

1. V. D. Belousov. *Foundations of Quasigroup and Loop Theory.* Nauka, Moscow, 1967. In Russian.

2. N. J. Cavenagh. The theory and application of latin bitrades: A survey. *Mathematica Slovaca*, 58(6):691–718, 2008. DOI: 10.2478/s12175-008-0103-2.

3. A. V. Cheremushkin. Canonical decomposition of n-ary quasigroups. volume 102 of *Mat. Issled.*, pages 97–105. Shtiintsa, Kishinev, 1988. In Russian.

4. D. S. Krotov and V. N. Potapov. n-Ary quasigroups of order 4. *SIAM J. Discrete Math.*, 23(2):561–570, 2009. DOI: 10.1137/070697331.

5. D. S. Krotov, V. N. Potapov, and P. V. Sokolova. On reconstructing reducible n-ary quasigroups and switching subquasigroups. *Quasigroups Relat. Syst.*, 16(1):55–67, 2008.

6. B. D. McKay and I. M. Wanless. On the number of Latin squares. *Ann. Comb.*, 9(3):335–334, 2005. DOI: 10.1007/s00026-005-0261-7.

7. B. D. McKay and I. M. Wanless. A census of small Latin hypercubes. *SIAM J. Discrete Math.*, 22(2):719–736, 2008. DOI: 10.1137/070693874.

8. V. N. Potapov. An upper estimation of the number of n-quasigroups of finite order. In *Proceedings of the XVII International School-Seminar "Synthesis and Complexity of Controlling Systems"*, pages 136–137, Novosibirsk, Russia, October–November 2008. In Russian.

9. V. N. Potapov and D. S. Krotov. Asymptotics for the number of n-quasigroups of order 4. *Sib. Math. J.*, 47(4):720–731, 2006. DOI: 10.1007/s11202-006-0083-9 translated from Sib. Mat. Zh. 47(4) (2006), 873-887.

Vladimir Potapov, Denis Krotov
Sobolev Institute of Mathematics,
prospekt Akademika Koptyuga 4, Novosibirsk 630090, Russia
and
Mechanics and Mathematics Department of the Novosibirsk State University,
Pirogova 2, Novosibirsk 630090, Russia

tel. +7-383-3634549, +7-383-3634666
vpotapov@math.nsc.ru, krotov@math.nsc.ru

О числе n-арных квазигрупп конечного порядка
On the number of n-ary quasigroups of finite order*

В. Н. Потапов*, Д. С. Кротов*

*Институт математики им. С. Л. Соболева СО РАН, проспект Академика Коптюга 4, Новосибирск

Механико-математический факультет, Новосибирский государственный университет, ул. Пирогова 2, Новосибирск

Аннотация

Пусть $Q(n,k)$ — число n-арных квазигрупп порядка k. Получена рекуррентная формула для чисел $Q(n,4)$. Доказано, что при любых $n \geq 2$ и $k \geq 5$ справедливы неравенства $\left(\frac{k-3}{2}\right)^{\frac{n}{2}} \left(\frac{k-1}{2}\right)^{\frac{n}{2}} < \log_2 Q(n,k) \leq c_k(k-2)^n$, где c_k не зависит от n. Таким образом, верхняя асимтотическая граница для чисел $Q(n,k)$ улучшена при любых $k \geq 5$, нижняя — при нечётных $k \geq 7$.

Let $Q(n,k)$ be the number of n-ary quasigroups of order k. We derive a recurrent formula for $Q(n,4)$. We prove that for all $n \geq 2$ and $k \geq 5$ the following inequalities hold: $\left(\frac{k-3}{2}\right)^{\frac{n}{2}} \left(\frac{k-1}{2}\right)^{\frac{n}{2}} < \log_2 Q(n,k) \leq c_k(k-2)^n$, where c_k does not depend on n. So, the upper asymptotic bound for $Q(n,k)$ is improved for any $k \geq 5$ and the lower bound is improved for odd $k \geq 7$.

Ключевые слова: n-арная квазигруппа, латинский куб, лупа, асимптотика, компонента, латинский трэйд.

Keywords: n-ary quasigroup, latin cube, loop, asymptotic estimate, component, latin trade.

УДК: 519.143
MSC2010: 20N15, 05B15

1. Введение

Алгебраическая система из множества Σ мощности $|\Sigma| = k$ и n-арной операции $f : \Sigma^n \to \Sigma$ называется n-арной квазигруппой порядка k, если унарная операция, полученная фиксацией любых $n-1$ аргументов операции f любыми значениями из Σ, всегда является биекцией. Принято называть *n-арной квазигруппой порядка k* или *n-квазигруппой порядка k* также и соответствующую функцию f (таблица значений такой функции известна под названием *латинский гиперкуб*, в случае $n = 2$ — *латинский квадрат*).

Зафиксируем множество элементов $\Sigma = \{0, 1, \ldots, k-1\}$. Обозначим через $Q(n,k)$ число различных n-арных квазигрупп порядка k (при фиксированном Σ)[1]. Известно, что для

*Работа выполнена при поддержке ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № 02.740.11.0429) и Российского фонда фундаментальных исследований (проекты 08-01-00671, 08-01-00673).

[1]Иногда под числом квазигрупп подразумевают число попарно неизоморфных квазигрупп.

каждого n существует только две n-арных квазигруппы порядка 2. Имеется $Q(n,3) = 3 \cdot 2^n$ различных n-арных квазигрупп порядка 3, которые составляют единственный класс эквивалентности. В [1] доказано асимптотическое равенство $Q(n,4) = 3^{n+1}2^{2^n+1}(1+o(1))$ при $n \to \infty$. В настоящей работе (раздел 4) предложен рекуррентный способ вычисления чисел $Q(n,4)$, выписаны первые 8 значений этой величины. Ранее были известны только пять первых значений $Q(n,4)$, кроме того, известны числа $Q(n,5)$ и $Q(n,6)$ для $n \leq 5$ и $n \leq 3$ соответственно, см. [9], и число $Q(2,k)$ при $k \leq 11$, см. работу [8] и библиографию в ней.

Асимптотика числа и даже логарифма числа (и даже логарифма логарифма числа) n-арных квазигрупп порядков больше 4 неизвестна. В [7] получены следующие нижние оценки $Q(n,5) \geq 2^{3^{n/3-c}}$, где $c < 0.072$; $Q(n,k) \geq 2^{(k/2)^n}$ если k чётно; $Q(n,k) \geq 2^{n(k/3)^n}$ если k кратно трём; $Q(n,k) \geq 2^{1.5\lfloor k/3 \rfloor^n}$ для произвольного k. В [4] была предложена верхняя оценка числа n-арных квазигрупп порядка k: $Q(n,k) \leq 3^{(k-2)^n}2^{n(k-2)^{n-1}}$.

В настоящей статье усилена верхняя оценка (раздел 2) числа n-арных квазигрупп конечного порядка и нижняя оценка (раздел 3) числа n-арных квазигрупп нечётного порядка:

$$\left(\frac{k-3}{2}\right)^{\frac{n}{2}} \left(\frac{k-1}{2}\right)^{\frac{n}{2}} < \log_2 Q(n,k) \leq c_k(k-2)^n,$$

где c_k не зависит от n, точнее, $c_k = \frac{\log_2 k!}{k-2} + \frac{k}{k-4}$.

2. Верхняя оценка

Будем говорить, что множество $M \subseteq \Sigma^n$ удовлетворяет свойству (A), если для любого элемента $\bar{x}$ из M и каждой позиции $i = 1, \ldots, n$ найдется другой элемент $\bar{y}$ из M, отличающийся от $\bar{x}$ только в позиции i. По индукции легко получить следующее:

Предложение 1. *Любое непустое подмножество $C \subseteq \Sigma^n$, удовлетворяющее свойству (A), имеет мощность не менее 2^n.*

Частичной n-арной квазигруппой порядка $|\Sigma|$ называется функция $g : \Omega \to \Sigma$, где $\Omega \subset \Sigma^n$, удовлетворяющая следующему свойству: $g(\overline{x}) \neq g(\overline{y})$ для любых двух наборов $\overline{x}, \overline{y} \in \Omega$, отличающихся ровно в одной позиции. Будем говорить, что n-арная квазигруппа $f : \Sigma^n \to \Sigma$ является *продолжением* частичной n-арной квазигруппы $g : \Omega \to \Sigma$, где $\Omega \subset \Sigma^n$, если $f|_\Omega \equiv g$.

Лемма 1. *Пусть $|\Sigma| = k$, $B = \Sigma \setminus \{a,b\}$, $k \geq 3$, $a, b \in \Sigma$. Тогда частичная n-арная квазигруппа $g : \Sigma^{n-1} \times B \to \Sigma$ имеет не более чем $2^{(k/2)^{n-1}}$ различных продолжений.*

Доказательство.

Пусть P — множество неупорядоченных пар элементов множества Σ. Рассмотрим частичную n-арную квазигруппу $g : \Sigma^{n-1} \times B \to \Sigma$. Определим функцию $G : \Sigma^{n-1} \to P$ равенством $G(\overline{x}) = \Sigma \setminus \{g(\overline{x}c) : c \in \Sigma \setminus \{a,b\}\}$. Определим граф $\Gamma = \langle \Sigma^{n-1}, E \rangle$, в котором две вершины $\overline{x}$ и $\overline{y}$ соединены ребром тогда и только тогда, когда наборы $\overline{x}$ и $\overline{y}$ отличаются только в одной позиции и $G(\overline{x}) \cap G(\overline{y}) \neq \varnothing$. Нетрудно видеть, что компоненты связности графа Γ удовлетворяют свойству (A).

Пусть n-арные квазигруппы f_1 и f_2 являются продолжениями частичной n-арной квазигруппы g. Нетрудно видеть, что $\{f_1(\overline{x}a), f_1(\overline{x}b)\} = G(\overline{x})$ для любого $\overline{x} \in \Sigma^{n-1}$, причём если $f_1(\overline{x}a) = f_2(\overline{x}a)$, то продолжения f_1 и f_2 совпадают на всей компоненте связности графа Γ, содержащей вершину $\overline{x} \in \Sigma^{n-1}$. Таким образом, для однозначного определения продолжения частичной n-арной квазигруппы g достаточно зафиксировать одно из двух возможных

значений в каждой компоненте связности графа Γ. Из предложения 1 следует, что каждая компонента связности имеет мощность не менее 2^{n-1}. Тогда число компонент связности графа Γ не превосходит $(k/2)^{n-1}$. А значит, g имеет не более $2^{(k/2)^{n-1}}$ продолжений. ▲

Теорема 1. *Если $k \geq 5$ и $n \geq 2$, то $Q(n,k) \leq 2^{c_k(k-2)^n}$, где $c_k = \frac{\log_2 k!}{k-2} + \frac{k}{k-4}$.*

Доказательство. Число частичных n-арных квазигрупп $g : \Sigma^{n-1} \times B \to \Sigma$, где $|\Sigma| = k$, $B = \Sigma \setminus \{a,b\}$ не превосходит $Q(n,k)^{k-2}$. Из леммы 1 следует неравенство

$$Q(n+1,k) \leq Q(n,k)^{k-2} 2^{(k/2)^n}. \tag{1}$$

Введём обозначение $\alpha_n = \log_2 Q(n,k)/(k-2)^n$. Тогда из неравенства (1) имеем

$$\alpha_{n+1} \leq \alpha_n + \left(\frac{k}{2(k-2)}\right)^n.$$

Поскольку $\alpha_1 = \frac{\log_2 k!}{k-2}$ и $\sum\limits_{n=1}^{\infty} \left(\frac{k}{2(k-2)}\right)^n = \frac{k}{k-4}$, имеем $\alpha_n \leq \frac{\log_2 k!}{k-2} + \frac{k}{k-4}$. ▲

3. Нижняя оценка

Пусть a и b — два различных элемента из Σ. *$\{a,b\}$-Компонентой* n-арной квазигруппы f будем называть такое множество $S \subset \Sigma^n$, что 1) $f(S) = \{a,b\}$ и 2) функция

$$g(\bar{x}) = \begin{cases} f(\bar{x}) & \text{при } \bar{x} \notin S, \\ b & \text{при } \bar{x} \in S \text{ и } f(\bar{x}) = a, \\ a & \text{при } \bar{x} \in S \text{ и } f(\bar{x}) = b. \end{cases}$$

также является n-арной квазигруппой. В этом случае будем говорить, что g получена из f *свитчингом* компоненты S. Заметим, что в определении $\{a,b\}$-компоненты условие 2) можно заменить свойством (A) из предыдущего раздела. Очевидно, что свитчинг непересекающихся компонент можно производить независимо:

Предложение 2. *Пусть S и S' — непересекающиеся $\{a,b\}$- и $\{c,d\}$- (соответственно) компоненты n-арной квазигруппы f и n-арная квазигруппа g получена из f свитчингом компоненты S. Тогда S' также является $\{c,d\}$-компонентой квазигруппы g.*

Следующее предложение нетрудно получить из определения $\{a,b\}$-компоненты, аналогичное утверждение имеется в [7].

Предложение 3. *Пусть множество $C = \{c_1,d_1\} \times \{c_2,d_2\}$ является $\{a,b\}$-компонентой 2-квазигруппы g. Пусть множество C_i является $\{c_i,d_i\}$-компонентой n_i-арной квазигруппы q_i при $i = 1,2$. Тогда множество $C_1 \times C_2$ является $\{a,b\}$-компонентой (n_1+n_2)-арной квазигруппы f, где $f(\bar{x}_1,\bar{x}_2) \equiv g(q_1(\bar{x}_1), q_2(\bar{x}_2))$.*

2-Квазигруппа $\varphi : \Sigma \to \Sigma$ называется *идемпотентной*, если $\varphi(x,x) = x$ для любого $x \in \Sigma$. Известно (см., например, [2]), что верно

Предложение 4. *Для любого $m \geq 3$ имеется идемпотентная 2-квазигруппа порядка m.*

В следующем предложении приведена конструкция 2-квазигрупп, которая будет использована при доказательстве нижней оценки числа n-арных квазигрупп нечётного порядка.

Предложение 5. *Для любого $m \geq 3$ найдётся 2-квазигруппа ψ порядка $2m+1$, имеющая m $\{2i,2i+1\}$-компонент для каждого $i \in \{0,\ldots,m-1\}$, причём все кроме одной $\{2i,2i+1\}$-компоненты имеют вид $\{2j,2j+1\} \times \{2l,2l+1\}$.*

Доказательство. По предложению 4 найдётся идемпотентная 2-квазигруппа φ_m порядка m. Для любых $a, b \in \{0, \dots, m-1\}$, $a \neq b$, и $\delta, \sigma \in \{0, 1\}$ определим

$\psi(2a+\delta, 2b+\sigma) = 2\varphi_m(a,b) + (\delta + \sigma \bmod 2)$;

$\psi(2a+\delta, 2a+\delta) = 2a+1-\delta$;

$\psi(2a+\delta, 2a+1-\delta) = k-1$;

$\psi(k-1, 2a+\delta) = \psi(2a+\delta, k-1) = 2a+\delta$;

$\psi(k-1, k-1) = k-1$.

Непосредственная проверка показывает, что ψ есть 2-квазигруппа, обладающая требуемыми свойствами. ▲

Ниже приведён пример таблиц значений 2-квазигруппы φ_4 и соответствующей ψ:

φ_4 :

0	2	3	1
3	1	0	2
1	3	2	0
2	0	1	3

ψ :

1	8	4	5	6	7	2	3	0
8	0	5	4	7	6	3	2	1
6	7	3	8	0	1	4	5	2
7	6	8	2	1	0	5	4	3
2	3	6	7	5	8	0	1	4
3	2	7	6	8	4	1	0	5
4	5	0	1	2	3	7	8	6
5	4	1	0	3	2	8	6	7
0	1	2	3	4	5	6	7	8

Из предложения 1 нетрудно заключить, что 2-квазигруппа нечётного порядка k, построенная в предложении 5, имеет максимальное число непересекающихся компонент среди всех 2-квазигрупп порядка k.

Теорема 2. *Если $k \geq 5$ — нечётное и $n \geq 2$, то*

$$Q(n,k) \geq 2^{\left(\frac{k-3}{2}\right)^{\left\lfloor \frac{n-1}{2} \right\rfloor} \left(\frac{k-1}{2}\right)^{\left\lceil \frac{n+1}{2} \right\rceil}} > 2^{\left(\frac{k-3}{2}\right)^{n/2} \left(\frac{k-1}{2}\right)^{n/2}}.$$

Доказательство. Пусть ψ – 2-квазигруппа порядка k, построенная в предложении 5. Определим рекуррентно n-арную квазигруппу Ψ^n равенствами:

$\Psi^2 \equiv \psi$;

$\Psi^{2m+1}(\overline{x}, y) = \psi(\Psi^{2m}(\overline{x}), y)$;

$\Psi^{2m+2}(\overline{x}, y, z) = \psi(\Psi^{2m}(\overline{x}), \psi(y, z))$.

Обозначим через α_n — число $\{2i, 2i+1\}$-компонент n-арной квазигруппы Ψ^n, где $i \in \{0, \dots, \frac{k-3}{2}\}$. Из предложений 3 и 5 имеем соотношения $\alpha_2 = \frac{k-1}{2}$, $\alpha_{2m+1} \geq \alpha_{2m} \frac{k-3}{2}$, $\alpha_{2m+2} \geq \alpha_{2m} \frac{k-3}{2} \frac{k-1}{2}$. Тогда $\alpha_{2m} \geq \left(\frac{k-3}{2}\right)^{m-1} \left(\frac{k-1}{2}\right)^m$ и $\alpha_{2m+1} \geq \left(\frac{k-3}{2}\right)^m \left(\frac{k-1}{2}\right)^m$.

Поскольку $\{2i, 2i+1\}$-компоненты при различных i не пересекаются, всего непересекающихся компонент не меньше, чем $\frac{k-1}{2}\alpha_n$. Из предложения 2 следует, что из n-арной квазигруппы Ψ^n свитчингами непересекающихся компонент можно получить требуемое число различных n-арных квазигрупп порядка k. ▲

4. Число n-арных квазигрупп порядка 4

Введём обозначение $[n] = \{1, \dots, n\}$. n-Арная квазигруппа f называется *n-арной лупой*, если существует такой элемент $e \in \Sigma$, называемый *единичным*, что для всех $i \in [n]$ и $a \in \Sigma$ имеет место равенство $f(e \dots \underset{i}{e a e} \dots e) = a$. Далее мы всегда будем подразумевать, что 0 является единичным элементом n-арной лупы (в общем случае могут быть и другие единичные элементы). Особо отметим, что данное соглашение существенно в интерпретации

понятия числа n-арных луп. В частности, имеем следующий простой и хорошо известный факт:

Предложение 6. *Пусть $Q'(n,k)$ — число n-арных луп порядка k. Тогда* $Q(n,k) = k \cdot ((k-1)!)^n Q'(n,k)$.

n-Арная квазигруппа f называется *разделимой (приводимой)*, если найдутся: целое число m, $2 \le m < n$, $(n-m+1)$-арная квазигруппа h, m-арная квазигруппа g и перестановка $\sigma : [n] \to [n]$ — такие, что

$$f(x_1, \ldots, x_n) \equiv h\left(g(x_{\sigma(1)}, \ldots, x_{\sigma(m)}), x_{\sigma(m+1)}, \ldots, x_{\sigma(n)}\right).$$

В дальнейшем будем предполагать, что $\Sigma = \{0,1,2,3\}$, т. е. речь пойдёт только об n-арных квазигруппах порядка 4. Известно (см., например, [2]), что имеется ровно четыре бинарные лупы порядка 4 (одна изоморфна группе $Z_2 \times Z_2$ и три — группе Z_4).

Следующее утверждение является прямым следствием теоремы из [3].

Лемма 2. *Для разделимой n-арной лупы f порядка 4 справедливо одно и только одно из двух представлений.*

$$f(\overline{x}) = q_0(q_1(\tilde{x}_1), ..., q_m(\tilde{x}_m)), \tag{2}$$

где q_j есть n_j-арные лупы при $j, 1 \le j \le m$, q_0 есть неразделимая m-арная лупа, $m \ge 3$, $\tilde{x}_j$ — некоторые наборы переменных x_i, $i \in I_j$, где $\{I_j\}$ — разбиение множества $[n]$. Причём в данном представлении разбиение $\{I_j\}$ единственно.

$$f(\overline{x}) = q_1(\tilde{x}_1) * ... * q_k(\tilde{x}_k), \tag{3}$$

где $*$ есть бинарная операция в одной из 4 луп, q_j есть n_j-арные лупы при $j, 1 \le j \le k$, непредставимые в виде $q_j(\tilde{x}_j) = q'(\tilde{x}'_j) * q''(\tilde{x}''_j)$, $\tilde{x}_j$ — некоторые наборы переменных x_i, $i \in I_j$, где $\{I_j\}$ — разбиение множества $[n]$. Причём в данном представлении разбиение $\{I_j\}$ единственно.

Корневой операцией n-арной квазигруппы f будем называть m-арную квазигруппу q_0, если имеет место представление (2), и бинарную операцию $*$, если имеет место представление (3).

Простой комбинаторный подсчёт показывает, что число $F_{\overline{j},\overline{k}}$ различных разбиений множества $[n]$ на k подмножеств, из которых k_i подмножеств имеет мощность j_i, $1 \le i \le t$, $0 < j_1 < \cdots < j_t$, удовлетворяет равенству

$$F_{\overline{j},\overline{k}} = \frac{n!}{(j_1!)^{k_1} \ldots (j_t!)^{k_t}} \frac{1}{k_1! \ldots k_t!}, \tag{4}$$

где $k_1 + k_2 + \cdots + k_t = k$, $k_1 j_1 + k_2 j_2 + \cdots + k_t j_t = n$.

Пусть $f : \Sigma^n \to \Sigma$ — n-арная квазигруппа, определим множество

$$S_{a,b}(f) \triangleq \{\bar{x} \in \Sigma^n : f(\bar{x}) \in \{a,b\}\}.$$

n-Арную лупу f назовём *a-полулинейной*, где $a \in \{1,2,3\}$ если характеристическая функция $\chi_{S_{0,a}(f)}$ множества $S = S_{0,a}(f)$ имеет вид

$$\chi_{S_{0,a}(f)}(x_1, \ldots, x_n) \equiv \sum_{i=1}^{n} \chi_{\{0,a\}}(x_i) \bmod 2. \tag{5}$$

n-Арная лупа f называется *линейной*, если она одновременно является a-полулинейной и b-полулинейной, где $a \neq b$, $a, b \in \{1, 2, 3\}$. Непосредственой проверкой нетрудно убедиться, что справедливо

Предложение 7. *Из четырёх бинарных луп порядка* 4 *одна (изоморфная группе* $Z_2 \times Z_2$*) является линейной, а три остальных* 1-, 2- *и* 3- *полулинейными соответственно.*

Известно (см. [1]), что

Предложение 8. *Линейная* n*-арная лупа единственна и является одновременно* 1-, 2- *и* 3- *полулинейной.*

Нетрудно видеть (см., также, [1]), что справедливо

Предложение 9. *Пусть* f *— разделимая* a*-полулинейная* n*-арная лупа, тогда* f *можно представить как суперпозицию* a*-полулинейных луп вида* (2) *или* (3).

Обозначим через ℓ_n^a мощность множества a-полулинейных n-арных луп и через ℓ_n мощность множества полулинейных n-арных луп.

Как было установлено в [1], мощность множества всех n-арных луп асимптотически совпадает с мощностью множества полулинейных n-арных луп, которая легко вычисляется:

Лемма 3 ([1]). $\ell_n = 3 \cdot 2^{2^n - n - 1} - 2$, $\ell_n^a = 2^{2^n - n - 1}$ *при* $a \in \{1, 2, 3\}$.

В [6] получено описание n-арных квазигрупп порядка 4 в определённых выше терминах, а именно, доказана

Теорема 3. *Каждая* n*-арная лупа порядка* 4 *является разделимой или полулинейной.*

На этом описании по-существу основывается вывод рекуррентной формулы для числа n-арных луп (и квазигрупп) порядка 4.

Введём следующие обозначения:

v_n — число n-арных луп (порядка 4);

r_n^* — число разделимых n-арных луп с бинарной корневой операцией $*$;

r_n^0 — число разделимых n-арных луп с корневой операцией арности большей либо равной 3;

r_n^{a*} — число разделимых a-полулинейных n-арных луп с a-полулинейной бинарной корневой операцией $*$;

r_n^{a0} — число разделимых a-полулинейных n-арных луп с корневой операцией арности большей либо равной 3;

p_n^a — число неразделимых a-полулинейных n-арных луп;

p_n — число неразделимых n-арных луп.

Из леммы 2 и предложения 9 вытекают следующие соотношения:

$$r_n^{a*} = \sum_{i=2}^{n} \sum_{\bar{j},\bar{k}} F_{\bar{j},\bar{k}} (\ell_{j_1}^a - r_{j_1}^{a*})^{k_1} \cdots (\ell_{j_t}^a - r_{j_t}^{a*})^{k_t},$$

$$r_n^* = \sum_{i=2}^{n} \sum_{\bar{j},\bar{k}} F_{\bar{j},\bar{k}} (v_{j_1} - r_{j_1}^*)^{k_1} \cdots (v_{j_t} - r_{j_t}^*)^{k_t},$$

$$r_n^{a0} = \sum_{i=3}^{n-1} p_i^a \sum_{\bar{j},\bar{k}} F_{\bar{j},\bar{k}} (\ell_{j_1}^a)^{k_1} \cdots (\ell_{j_t}^a)^{k_t},$$

$$r_n^0 = \sum_{i=3}^{n-1} p_i \sum_{\bar{j},\bar{k}} F_{\bar{j},\bar{k}} (v_{j_1})^{k_1} \cdots (v_{j_t})^{k_t},$$

где вторая сумма берётся по наборам $\bar{k} = (k_1, \ldots, k_t)$ и $\bar{j} = (j_1, \ldots, j_t)$ положительных целых чисел, удовлетворяющим равенствам $k_1 + \cdots + k_t = i$, $k_1 j_1 + k_2 j_2 + \cdots + k_t j_t = n$ и неравенствам $j_1 < \cdots < j_t$. Из теоремы 3 и предложения 8 вытекают соотношения $v_n = p_n + r_n^0 + 4r_n^*$, $p_n^a = \ell_n^a - r_n^{a0} - 2r_n^{a*}$, $p_n = 3p_n^a$. Из леммы 3 имеем $\ell_n^a = 2^{2^n - n - 1}$ при $a \in \{1, 2, 3\}$.

Из предложения 7 имеем начальные значения для перечисленных выше величин: $r_2^{a*} = 2$, r_2^*=4, $r_2^{a0} = r_2^0 = 0$. Нетрудно видеть, что приведённые выше равенства и предложение 6 обеспечивают рекуррентный способ вычисления числа n-арных квазигрупп порядка 4.

Наконец, выпишем первые восемь значений величины $Q'(n, 4)$: 1, 4, 64, 7132, 201538000, 432345572694417712, 39876839873547476429227735396327796 8, 67846927287489958255998624028528071036486706348977951042703872222975027683 2, — и величины $Q(n, 4)$: 24, 576, 55296, 36972288, 6268637952000, 80686060158523011084288, 44651852187365545446769179264602567250001 92, 45582713849161893490442953958520081824807862308417980087416842819065769 63885826048.

5. Заключение

В заключении скажем несколько слов о связи тематики настоящей статьи с известным понятием латинского трэйда (latin trade). Частичная n-арная квазигруппа $t : \Omega \to \Sigma$, $\Omega \subset \Sigma^n$ называется *многомерным латинским трэйдом*, далее просто *трэйдом*, если существует другая частичная n-арная квазигруппа $t' : \Omega \to \Sigma$ такая, что

1) $t(\bar{x}) \neq t'(\bar{x})$ для всех $\bar{x} \in \Omega$;

2) для любого i, $i = 1, \ldots, n$, и для любых допустимых значений $x_1, \ldots, x_{i-1}, x_{i-1}, \ldots, x_n$ множества $\{t(x_1, \ldots, x_{i-1}, y, x_{i-1}, \ldots, x_n) \mid y \in \Sigma\}$ и $\{t'(x_1, \ldots, x_{i-1}, y, x_{i-1}, \ldots, x_n) \mid y \in \Sigma\}$ совпадают.

В этом случае пара (t, t') называется *битрейдом* (в зависимости от контекста, битрейд рассматривают как упорядоченную, либо как неупорядоченную пару), а трэйд t' называется *партнёром* трэйда t. Исследованию битрэйдов в случае $n = 2$ (латинских битрэйдов) уделяется значительное внимание, см. обзор [5].

Будем говорить, что n-арная квазигруппа f содержит трэйд t, если $t = f|_\Omega$ для некоторого Ω. При этом из определений следует, что замена значений f на множестве Ω значениями партнёра t' трэйда t приводит к другой n-арной квазигруппе. Трэйды $t = f|_\Omega$ и $s = f|_\Theta$ назовём *независимыми*, если их носители (области определения) Ω и Θ не пересекаются. Максимальное число попарно независимых трэйдов, которые содержит n-арная квазигруппа f, назовём её *трэйдовым числом* $\mathrm{trd}(f)$. Максимум $\mathrm{trd}(f)$ по всем n-арным квазигруппам f порядка k обозначим через $\mathrm{Trd}(n, k)$. Поскольку независимые трэйды в n-арной квазигруппе можно независимо заменять на партнёров, число $Q(n, k)$ различных n-арных квазигрупп порядка k удовлетворяет неравенству

$$Q(n, k) \geq 2^{\mathrm{Trd}(n,k)}. \tag{6}$$

Легко понять, что нижняя оценка в разделе 3 (как и все оценки в [7]) получена именно таким образом: $\{a, b\}$-компонента по определению является носителем некоторого трэйда. Поскольку носитель трэйда обладает свойством (A), из предложения 1 вытекает $\mathrm{Trd}(n, k) \leq k^n/2^n = 2^{(\log_2 k - 1)n}$, причем для чётных k легко доказать равенство. Для нечётных k из результатов раздела 3 следует оценка $\mathrm{Trd}(n, k) \geq 2^{c(k)n}$, где $c(k) \underset{k\to\infty}{\longrightarrow} \log_2 k - 1$. Однако для

фиксированных k, в частности, для малых значений 5, 7, ... вопрос об асимптотическом поведении величины $\mathrm{Trd}(n,k)$ остаётся открытым.

Проблема 1. *Вычислить асимптотику логарифма и асимптотику величины* $\mathrm{Trd}(n,k)$ *при* $n \to \infty$ *для нечётных* $k \geq 5$.

Другой вопрос состоит в том, насколько оценка (6) близка к истинной. Для порядка 4 оценка (6) асимптотически точна после логарифмирования. Для большего фиксированного порядка асимптотика двукратного логарифма величины $Q(n,k)$ неизвестна. Кажется естественным предположить, что асимптотика двукратного логарифма величины $Q(n,k)$ и логарифма величины $\mathrm{Trd}(n,k)$ совпадают.

Проблема 2. *Верно ли, что* $\lim\limits_{n\to\infty}\left(\frac{\log_2\log_2 Q(n,k)}{n}\right) = \lim\limits_{n\to\infty}\left(\frac{\log_2 \mathrm{Trd}(n,k)}{n}\right)$*? В частности, верно ли, что* $\lim\limits_{n\to\infty}\left(\frac{\log_2\log_2 Q(n,k)}{n}\right) \leq \log_2 k - 1$*?*

Существование этих пределов также не доказано.

Список литературы

1. *Потапов В. Н., Кротов Д. С.* Асимптотика числа n-квазигрупп порядка 4 // *Сибирский математический журнал.* — 2006. — Т. 47, № 4. — С. 873–887.

2. *Белоусов В. Д.* Основы теории квазигрупп и луп. — Москва: Наука, 1967.

3. *Черемушкин А. В.* Каноническая декомпозиция n-арных квазигрупп. — Кишинев: Штиинца, 1988. — Т. 102 из *Мат. Исслед.* — С. 97–105.

4. *Потапов В. Н.* Верхняя оценка числа n-квазигрупп конечного порядка // Труды XVII международной школы-семинара "Синтез и сложность управляющих систем". — Новосибирск, Россия: 2008. — октябрь–ноябрь. — С. 136–137.

5. *Cavenagh N. J.* The theory and application of latin bitrades: A survey // *Mathematica Slovaca.* — 2008. — Vol. 58, no. 6. — Pp. 691–718. — DOI: 10.2478/s12175-008-0103-2.

6. *Krotov D. S., Potapov V. N.* n-Ary quasigroups of order 4 // *SIAM J. Discrete Math.* — 2009. — Vol. 23, no. 2. — Pp. 561–570. — DOI: 10.1137/070697331.

7. *Krotov D. S., Potapov V. N., Sokolova P. V.* On reconstructing reducible n-ary quasigroups and switching subquasigroups // *Quasigroups Relat. Syst.* — 2008. — Vol. 16, no. 1. — Pp. 55–67.

8. *McKay B. D., Wanless I. M.* On the number of Latin squares // *Ann. Comb.* — 2005. — Vol. 9, no. 3. — Pp. 335–334. — DOI: 10.1007/s00026-005-0261-7.

9. *McKay B. D., Wanless I. M.* A census of small Latin hypercubes // *SIAM J. Discrete Math.* — 2008. — Vol. 22, no. 2. — Pp. 719–736. — DOI: 10.1137/070693874.

Потапов Владимир Николаевич, Кротов Денис Станиславович
Институт математики им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4, Новосибирск 630090
тел. 383-3634549, 383-3634666
vpotapov@math.nsc.ru, krotov@math.nsc.ru